Department of Homeland Security Daily Open Source Infrastructure Report for 07 April 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Officials from the Department of Homeland Security, Department of Justice, Department of Labor, Department of State and other agencies have announced the creation of task forces in 10 major U.S. cities to combat the growing problems of document fraud and immigration benefits fraud. (See item 8)
- The Associated Press reports a Swedish man pleaded guilty to trying to carry a machete on an airplane and was given a six−month suspended sentence and ordered to surrender his weapon. (See item 13)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *April 05, Agence France−Presse* — **Kuwait prequalifies 11 foreign companies for new refinery.** Kuwait has prequalified 11 international companies for the construction of a new $6.3 billion oil refinery with a capacity of more than 600,000 barrels per day (bpd). Kuwait National Petroleum Co, which owns all Kuwaiti refineries, said the project has been divided into four major contracts. The prequalified companies include Korean Hyundai Engineering and Construction Co., US Stone and Webster International Inc., and United Arab Emirates−based Petrofac International Ltd. The refinery will be built in Al−Zour area, 60 miles south of the

capital near the border with Saudi Arabia. The project is planned to be completed in early 2010. Kuwait has 10 percent of the world's proven oil reserves and currently produces 2.6 million bpd of crude oil at full capacity. Kuwait plans to invest up to 40 billion dollars in the next 15 years to modernize its oil sector which generates more than 90 percent of public revenue. The emirate seeks to increase its output capacity to four million bpd by 2020.
Source: http://news.yahoo.com/s/afp/20060405/wl_mideast_afp/kuwaitoilrefinery_060405132607

2. *April 05, Utility Automation & Engineering* — **EPRI pinpoints cause of transformer failures.** Engineers at EPRI Solutions have conclusively identified the root cause of a number of recent failures in large power transformers owned by electric utilities. These and similar failures, reported in several countries around the world, have puzzled owners and manufacturers alike, particularly since many of the problems have occurred in equipment that was relatively new. Many of the transformer failures are attributable to corrosive sulfur contamination in the electrical insulating oils, according to EPRI Solutions' Nick Abi−Samra. He said, "We've found that the failures are not confined to any certain transformer manufacturers or oil suppliers. Even though the transformer oils have passed industry specifications and standard tests, many of them contain thermally unstable sulfur−bearing compounds...These compounds can be converted to corrosive sulfur as the equipment operates under heavy load, so generator step−up transformers and other transformers that operate consistently at high temperatures are at the greatest risk of failure."
Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICLE_ID=252038&p=22

3. *April 05, Reuters* — **U.S. needs more LNG imports to meet gas demand.** The United States needs to build more terminals to handle imports of super−cooled liquefied natural gas to help meet future demand and reduce gas prices, an industry report said on Wednesday, April 5. With many federal lands and offshore areas that hold huge gas reserves off limits to drilling and an Alaskan gas pipeline not expected to be ready for a decade, the United States will have to rely more on LNG imports to meet demand. "LNG is our best hope for adding measurably to U.S. gas supplies in the short to medium term," according to the report from the Manufacturers Alliance/MAPI, which represents major natural gas consuming companies. There are four U.S. LNG terminals operating onshore and one offshore deepwater port that handled about 631 billion cubic feet in LNG imports last year. Three import terminals are under construction and nine other terminals have been approved by federal regulators. If those 12 terminals are completed, total U.S. LNG import capacity would rise to almost five trillion cubic feet by 2010, which would be equal to 21 percent of projected U.S. gas demand at the time, the report said.
Source: http://today.reuters.com/News/CrisesArticle.aspx?storyId=N05 336577

4. *April 05, Contra Costa Times (CA)* — **Pacific Gas & Electric powers up to serve more.** A post−energy crisis lull in the construction of new power plants in Northern California neared an end Tuesday, April 4, as PG&E Corp. announced $1.5 billion in development deals that could provide it with 1,780 megawatts −− enough new electricity to serve 1.4 million households. The deals mark "a momentous step to secure new, clean and reliable electricity suppliers to power California's growing economy and replace an aging fleet of power plants," Tom King of PG&E's utility unit, said. PG&E also has in the works a $380 million deal to acquire and complete a 40 percent constructed, 530−megawatt power plant in Antioch from Mirant Corp. The deals would leave PG&E owning two new power plants and holding long−term contracts

for the output of three other plants owned by third parties. All of the deals require approval by state regulators. California officials have ambitious targets to increase use of renewable fuels. PG&E's announcement acknowledged those goals, noting that it expects to line up 1,500 megawatts of electricity generated from renewables in the next five years, and that it would invest an additional $1 billion of money from ratepayers in conservation efforts expected to reduce demand by 1,000 megawatts.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8knpp%5E%5BglpsrouZSigt9K%22bfel%5Dv

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *April 05, Government Accountability Office* — **GAO−06−409T: Defense Acquisitions: DoD Wastes Billions of Dollars through Poorly Structured Incentives (Testimony).** With the Department of Defense (DoD) spending over $200 billion annually to acquire products and services that include everything from spare parts to the development of major weapon systems, our numerous, large, and mounting fiscal challenges demand that DoD maximize its return on investment and provide the warfighter with needed capabilities at the best value for the taxpayer. In an effort to encourage defense contractors to perform in an innovative, efficient, and effective way, DoD gives its contractors the opportunity to collectively earn billions of dollars through monetary incentives known as award and incentive fees. Using these incentives properly −− in concert with good acquisition practices −− is a key to minimizing waste, maximizing value, and getting our military personnel what they need, when and where they need it. The subcommittee asked the Government Accountability Office (GAO) to testify on DoD's use of award and incentive fees and the role they play in the acquisition system. This statement highlights the risks of conducting business as usual and identifies the actions DoD needs to take to use these fees more effectively. DoD partially concurred with the seven recommendations GAO made in a previously issued report on award and incentive fees.
Highlights: http://www.gao.gov/highlights/d06409thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−409T

[Return to top]

Banking and Finance Sector

6. *April 07, Vermont Press Bureau* — **Vermont State College narrows down personal data exposed by laptop theft.** A month after the theft of a laptop computer containing personal information of thousands of students and employees of the Vermont State Colleges (VSC) system, officials are narrowing down the types of private information that were exposed. In an e−mail sent Monday, April 3 to students, faculty, staff, and alumni of the five state colleges,

VSC Chancellor Robert Clarke emphasized the colleges' assertion that no personal information has been accessed or compromised from the laptop, which has not been recovered. The concealed laptop was stolen February 28 from the chief information officer's car while it was parked on the streets of Montreal. Clarke said the colleges' notified all banks in Vermont, New Hampshire, and New York on Monday, March 27 of the theft and potential release of financial information. Employee information from June 2002 to November 2005 may have been archived on the laptop. The data, which includes names, addresses, Social Security numbers, salary, taxes, withholding and wage garnishment information, and bank account numbers, were not encrypted. Admissions information for all students from June 2002 to December 2004 could have been on the computer.
Source: http://www.timesargus.com/apps/pbcs.dll/article?AID=/RH/20060406/NEWS/604060353/1004/EDUCATION05

7. *April 06, Bank of New Zealand* — **Bank of New Zealand announces additional ATM security measure.** Bank of New Zealand has commenced the installation of security devices on its ATM machines nationally as an additional security precaution against ATM skimming fraud. The security device, known as a “green sleeve” due to its distinctive coloring, makes it difficult to fit a skimming device over the ATM card reader, while a hologram embedded in the sleeve inhibits replication of the device. The move follows suspected ATM skimming incidents last month at two Bank of New Zealand ATM machines. To date, fraud arising from these incidents is believed to amount to $54,690, with 38 cards believed to have been compromised. No new incidents of fraud have been detected in recent days. Around 2000 Bank of New Zealand ATM cards were cancelled in a precautionary measure.
Source: http://www.scoop.co.nz/stories/PO0604/S00058.htm

8. *April 05, U.S. Immigration and Customs Enforcement* — **Joint task forces created in 10 cities to combat document and benefit fraud.** Officials from the Department of Homeland Security, Department of Justice, Department of Labor, Department of State and other agencies announced the creation of task forces in 10 major U.S. cities to combat the growing problems of document fraud and immigration benefits fraud. The new “Document and Benefit Fraud Task Forces” will build upon the success of an existing task force in the Washington, DC / northern Virginia area. Led by U.S. Immigration and Customs Enforcement (ICE), a team of agents will partner with U.S. Attorney's Offices to formulate a comprehensive approach in targeting criminal organizations behind these schemes as well as the ineligible beneficiaries of such fraud. Any case where a sufficient nexus to terrorism is discovered will be referred to the Joint Terrorism Task Forces. The task forces will primarily target document fraud, which includes the manufacture, sale, or use of counterfeit identity documents −− such as fake driver's licenses, birth certificates, social security cards, or passports −− for immigration fraud or other criminal activity; and benefit fraud, which is the misrepresentation or omission of material fact on an application to obtain an immigration benefit one is not entitled to.
Source: http://www.ice.gov/graphics/news/newsreleases/articles/06040 5dc.htm

9. *April 05, BBC* — **Few users know how to spot phishing Websites.** An academic study looked at whether Web users could tell legitimate online bank Websites from the fakes produced by phishers. Though many phishing sites were easy to spot, the best were judged real by almost all participants. The study, conducted by researchers at Harvard and the University of California−Berkeley, found that users ignored most of the visual cues on browsers that warn

people that they are being scammed. The study looked at bogus Websites created by phishing gangs and what made users believe that these sites were legitimate. The study presented real online banking and fake phishing sites to subjects to see if they could tell the two types apart. On average, 40 percent of users failed to spot the phishing sites. The study revealed that people were caught out because they were generally ignorant about what did, and did not, indicate that a site was legitimate. For instance, few of those participating looked at the domain name displayed in a browser address bar. Users generally did not look at the address bar, status bar, or other security indicators. Many participants also ignored more direct warnings contained in pop−up windows that a site may not be legitimate.
Source: http://news.bbc.co.uk/2/hi/technology/4879468.stm

10. *April 05, WPBF 25 (FL)* — **Police target check−counterfeiting ring.** An organized crime ring is forging thousands of dollars in paychecks, forcing some stores to stop cashing checks and putting a strain on area migrant workers, police said. At least $60,000 in forged payroll checks has been cashed at six Palm Beach County, FL businesses and a local bank. A professional crime organization is behind the counterfeiting scheme that targets local firms and stores that cater to migrant workers. Detectives suspect that the group of 10 to 15 Hispanic men conspired in the check−cashing scheme. The well−planned scam is hard to detect. One of the men who works at a local farm sends his paycheck to his co−conspirators, who send it out of the country where the check is re−printed. Then, they take the pictures of the men who are going to cash the checks and come up with two fake names and two fake resident alien cards for each of them, and put several checks into two envelopes and mail them back. When another payday arrives, the fake workers with the fake checks go to the store with the migrant workers and cash the checks.
Source: http://news.yahoo.com/s/wpbf/20060405/lo_wpbf/3377975

[Return to top]

Transportation and Border Security Sector

11. *April 06, Reuters* — **U.S. airlines' strong revenue outweighs oil, for now.** U.S. airlines' strong revenue gains have turned previously gloomy investors more hopeful that the industry could return to profit, but resurgent fuel prices remain a potential spoiler, analysts said. By slashing employee pay and other costs, U.S. carriers have reduced billions of dollars in losses triggered by earlier oil price surges that sent some into bankruptcy. Lately, improved pricing power, bolstered by strong demand combined with cutbacks in available seats, has given a big boost to revenue as well. But oil prices −− the sector's main nemesis in recent years −− still loom as a threat. "Higher fares are helping, but I'd become more concerned if (oil) goes over $70 and stays there," said Ray Neidl, an analyst with Calyon Securities. "If we get back into the $70s and stay there it obviously throws our model," said Jim Corridore, an analyst at Standard & Poor's, who added that his forecasts call for oil prices for the full year in a range of $58 to $60 a barrel. While U.S. airlines this year have increased their purchases of contracts that lock in fuel at fixed prices, hedging is still not widespread enough to protect most airlines from a crude oil price spike at or above $70, analysts said.
Source: http://www.usatoday.com/travel/flights/2006−04−05−airline−in dustry−outlook_x.htm

12.

April 06, Tampa Bay Business Journal (FL) — **Tampa Bay Business Journal: Tampa Port Authority discusses $1 million master plan study.** The Tampa Port Authority board of commissioners held a public workshop Thursday, April 6, to discuss and obtain input on the port's master plan, which is currently being formulated. It's the first part of a $1 million study that will determine what the port should look like in 10 to 20 years. The profile of the economic benefits that the port generates is changing, Michael G. Horton, vice president of ports at Moffatt & Nichol said. "There is major opportunity to expand into the container and distribution markets," he said. The next stage of the study, out in the next six to eight weeks, will address the needs, access impacts, alternatives, benefits and costs of the existing and new markets, and translate those market opportunities into physical requirements and benefits to the community, said Horton.
Source: http://tampabay.bizjournals.com/tampabay/stories/2006/04/03/ daily60.html

13. *April 06, Associated Press* — **Swedish man pleads guilty to trying to take machete on plane.** A Swedish man pleaded guilty to trying to carry a machete on an airplane and was given a six−month suspended sentence and ordered to surrender his weapon. Peter Svenberg, who was in the country to make welding repairs at a Stevenson, AL, paper mill, was arrested March 29 at Chattanooga Metropolitan Airport. Authorities say Svenberg had the knife in luggage that he tried to take on the plane. His bond was set at $5,000, but immigration officials said he was a flight risk, and Svenberg was held seven days in the Hamilton County, TN, jail. Svenberg, 34, pleaded guilty to the charges Wednesday, April 5, in General Sessions Court and was expected to leave for Sweden on Thursday, April 6. A spokesperson for the U.S. Immigration and Customs Enforcement said he was looking into the matter.
Source: http://www.al.com/newsflash/regional/index.ssf?/base/news−20 /1144350557223020.xml&storylist=alabamanews

14. *April 06, Associated Press* — **Flight attendants object to NWA price plan.** Flight attendants at Northwest Airlines Corp. (NWA) are raising safety concerns about the airline's program to sell exit−row seats with extra legroom to passengers willing to pay a $15 fee. The Professional Flight Attendants Association sent a letter to Northwest Chief Executive Doug Steenland calling the idea "ill conceived," alleging it degrades federal safety rules about who can sit in the exit row. Passengers who sit in exit−rows must be at least 15 years old and be willing and able to help with the emergency evacuation of the aircraft, including opening the emergency door. NWA passengers who pay to reserve one of the seats online or at a kiosk check a box indicating they accept the conditions. The process has been approved by the Federal Aviation Administration. Jeanne Elliott, the union's regulatory affairs coordinator, wrote, "It takes away from the safety aspect of why we have designated people in exit rows that are willing and able to assist the crew in a time of emergency." Eagan, MN−based Northwest, the nation's fourth−largest airline, has been operating under Chapter 11 bankruptcy protection since September.
Source: http://biz.yahoo.com/ap/060406/northwest_premium_pricing.htm l?.v=2

15. *April 06, Telegraph News (UK)* — **Russian airline passengers face lie detector tests.** Millions of airline passengers traveling through Russia will soon have to take a lie detector test as part of new security measures. The technology, developed by an Israeli company, to be introduced at Moscow's Domodedovo airport as early as July, is intended to identify terrorists and drug smugglers. If successful, it could revolutionize check−ins. Passengers will pick up the handset

of a "truth verifier" machine while they are asked questions. "If a person fails, he is accompanied by a guard to a cubicle where he is asked questions in a more intense atmosphere," said Vladimir Kornilov, the IT director for East Line, which operates the airport.
Source: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/04/06/wlie06.xml&sSheet=/news/2006/04/06/ixnewstop.html

16. *April 05, Department of Transportation* — **FAA contract negotiations with NATCA reach impasse.** After receiving a “best and final” contract proposal more costly than what the air traffic controllers union indicated publicly last week, the U.S. Department of Transportation's Federal Aviation Administration (FAA) has ended contract negotiations with the National Air Traffic Controllers Association (NATCA). The union rejected an agency proposal that preserved the current salaries and benefits for the existing workforce while still saving taxpayers nearly $1.9 billion over the next five years. The FAA’s final offer was over $200 million better than its previous formal offer, all of that directed to preserving the annual cash compensation of the existing workforce. The FAA will submit its final proposal to Congress, which has 60 days to review the FAA’s proposal and NATCA’s objections. By statute, the FAA is authorized to implement its proposal if Congress does not act otherwise within the 60 days. With the help of a federal mediator, both sides agreed on the vast majority of the provisions in the contract. Negotiations stalled on the issue of base pay and two types of premium pay that together have escalated the average controller’s salary and benefits to over $170,000 annually, a more than 75 percent increase from 1998−2006.
Source: http://www.dot.gov/affairs/impasse.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

17. *April 06, Daily Citizen (WI)* — **Preparedness training held.** With agriculture playing a large economic role in Dodge, WI, a group of individuals gathered to learn how to prepare for an incident that would put the county's food supply at risk. Twenty−one emergency response officials, dairy processors, and health officials attended a session on agroterrorism preparedness training on Tuesday, April 4. During the session, attendees learned about understanding the potential affects of an agroterrorism attack, strategies for coordination among industry and local, state and federal entities and identifying individual roles within a response team.
Source: http://www.wiscnews.com/bdc/news/index.php?ntid=79186&ntpid= 2

18. *April 05, Animal and Plant Health Inspection Service* — **Availability of citrus canker scientific evaluation announced.** The U.S. Department of Agriculture’s Animal and Plant Health Inspection Service (APHIS) Wednesday, April 5, published for public comment the findings of its citrus canker evaluation, which concludes that asymptomatic fruit is an unlikely pathway for the further spread of the disease. Fruit that shows no signs of citrus canker is

referred to as asymptomatic fruit. The scientific evaluation affirms an underlying principle of the recently released draft Citrus Health Response Plan, that asymptomatic fruit does not pose a threat to other citrus producing areas because it does not further spread the disease. This finding is specific to commercially produced citrus fruit that has been treated with disinfectant dips and subjected to other mitigations. Even if infected fruit were to enter a citrus canker−free area with susceptible hosts, the evaluation found that the likelihood of establishment of the disease through this pathway is remote. The evaluation will now undergo a peer review to confirm these findings. According to the evaluation, even if viable disease−producing organisms were present, it is highly unlikely that the necessary environmental and physiological conditions for disease development would be present at the precise time infected citrus was placed in close proximity to a citrus tree.
Citrus Health Response Plan: http://www.aphis.usda.gov/ppq/pdmp/citrushealth/
Source: http://www.aphis.usda.gov/newsroom/content/2006/04/ccanker−e val_ppq.shtml

[Return to top]

Food Sector

19. *April 06, USAgNet* — **Beef giant buys four other companies.** Cargill Meat Solutions, of Wichita, KS, a leading U.S. beef, pork, and turkey processor, has completed the acquisition of four California−based meat companies: Beef Packers Inc., Fresno Meat Co., RPM Beef Inc., and King−O−Meat Inc. Beef Packers, Fresno Meat, RPM Beef, and King−O−Meat will be combined under one name: Beef Packers Inc.
Source: http://www.usagnet.com/story−national.cfm?Id=580&yr=2006

[Return to top]

Water Sector

20. *April 06, Hendersonville News (NC)* — **Wastewater spills from sewer company.** The Etowah Sewer Co. had a wastewater overflow Saturday, April 1, at the Etowah, NC, Wastewater Treatment Plant's main influent lift station. The overflow is estimated to be about 12,000 gallons. It is estimated that as much as 10,000 gallons of the untreated wastewater may have drained to or near Gash Creek. The cause of the spill was an electrical malfunction that damaged the main pumps control circuitry.
Source: http://www.hendersonvillenews.com/apps/pbcs.dll/article?AID=/20060406/NEWS/604060353/1042/NEWS01

21. *April 03, U.S. Environmental Protection Agency* — **Environmental Protection Agency cites Lynchburg for chlorine release.** The U.S. Environmental Protection Agency (EPA) has filed an administrative complaint against the city of Lynchburg, VA, for failing to properly report a chlorine release from its wastewater treatment plant. EPA’s complaint, which seeks $56,680 in penalties, alleges the plant operators did not immediately notify federal authorities, as required under the Comprehensive Environmental Response Compensation and Liability Act (CERCLA), and did not provide a follow−up report in a timely manner after the release, as required by the Emergency Planning and Community Right−to−Know Act. According to the

complaint, approximately 1,958 pounds of chlorine were released from Lynchburg's wastewater treatment facility on May 17, 2005. Chlorine is considered a hazardous substance, and the facility is required to report any release of chlorine that exceeds the reportable quantity to the National Response Center (NRC) as soon as they are aware of the release. Under CERCLA, the reportable quantity for chlorine is 10 pounds. The release, which was nearly 200 times the reportable quantity, was not reported to the NRC until May 19, more than 36 hours after operators at the facility had knowledge of the release.
Source: http://yosemite.epa.gov/opa/admpress.nsf/93216b1c8fd122ca85257018004cb2dc/bd29f842ccaae9e585257145005ec704!OpenDocument

[Return to top]

Public Health Sector

22. *April 06, Agence France−Presse* — **Egypt struggles to combat spread of bird flu to humans.** Two more human cases of bird flu have been reported in Egypt, as health officials struggled to enforce preventive measures. The latest cases, reported by the official MENA news agency on Thursday, April 6, brought to 11 the number of human infections in the country, where two women have already died of the virus. Health Minister Hatem al−Gebali said the latest victims were a 16−year−old girl and an eight−year−old child from the northern provinces of Menufiya and Qalyubia. Egypt, where urban rooftop and backyard rearings are almost a part of national folklore, has slapped a ban on domestic poultry farms and more than 10 million birds are believed to have been slaughtered. While monitoring compliance with government measures is easier in large poultry farms, many Egyptians with small domestic farms have been reluctant to cull their birds.
Source: http://news.yahoo.com/s/afp/20060406/wl_mideast_afp/egypthealthflu_060406095758;_ylt=AnKGYLtIQKceaUyDiG3sqymJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

23. *April 06, New York Times* — **Britain confirms bird flu found in Scottish swan.** A swan found dead in eastern Scotland has tested positive for the H5N1 strain of bird flu, government officials said, making it the first recorded case of the disease in a wild bird in Great Britain. The bird, believed to be a native mute swan, was discovered eight days ago in the harbor at Cellardyke, a small coastal town in Fife, northeast of Edinburgh. Officials have established a 1.8−mile protection zone around the spot where the bird was found to prevent the movement of poultry in and out of the area.
Source: http://www.nytimes.com/2006/04/06/world/europe/06cnd−britain.html?_r=1&oref=slogin

24. *April 05, Agence France−Presse* — **France pushes ahead on vaccine, drug for island disease.** Health Minister Xavier Bertrand said that France was exploring two paths that could lead to a vaccine and treatment for chikungunya, the disabling mosquito−borne disease that has swept across the Indian Ocean island of Reunion. "We are going to work on quickly developing a vaccine," Bertrand said Wednesday, April 5, adding that U.S. experiments in a prototype vaccine had been highly promising. The U.S. vaccine was successfully tested in the 1980s for effectiveness on mice and lab monkeys and for safety on humans, but was put on hold before large−scale human trials could take place. Bertrand added that virologists at the Timone

Hospital in Marseille, southern France, had been asked to assess lab−dish evidence that a drug which is already licensed for parasitic infection also kills the virus that causes chikungunya. Overall some 230,000 people −− out of a total population of 777,000 −− have contracted chikungunya in the last year, of whom 174 have died directly or indirectly as a result of the disease, according to figures released Friday, March 31.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://news.yahoo.com/s/afp/20060405/hl_afp/francereunionhealthchikungunya_060405142243;_ylt=AgLSz.tGUh_ZJ2FuXjpL.nuJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

25. *April 06, Agence France−Presse* — **International anti−terror exercise opens in Australia.** An international anti−terror exercise began in northern Australia Wednesday, April 6. Australia, Britain, Japan, New Zealand, Singapore and the United States are taking part in the three−day exercise that simulates an air interception of weapons of mass destruction. The exercise is the sixth to take place as part of the Proliferation Security Initiative (PSI) launched by President George W. Bush in 2003. The PSI commits countries to disrupt trade in weapons of mass destruction by interdicting vessels, aircraft, or other modes of transport that are reasonably suspected of carrying suspicious cargo.
Source: http://www.defensenews.com/story.php?F=1669916&C=airwar

26. *April 06, Union Leader (NH)* — **Drill to test emergency plans in the event of radioactivity release.** An exercise Monday and Tuesday, April 10−11, will help test Seabrook Station's emergency plan and those of 17 New Hampshire cities and towns and six Massachusetts communities within 10 miles of the nuclear power plant. The exercise, called "Injection Pathway," will include addressing an "immediate emergency" scenario at the plant which results in the release of radioactivity into the atmosphere. In addition to evaluating communications capabilities, the exercise will analyze command and control issues. Other concerns include the accuracy of maps, how quickly public health teams are able to get into the field following an incident and how well state, federal and utility officials are able to communicate with the media, to get information to the public.
Source: http://www.unionleader.com/article.aspx?headline=Seabrook+drill+to+test+emergency+plans&articleId=6590087c−2c04−4abd−b18 c−b31bc2eab20d

27. *April 06, Government Accountability Office* — **GAO−06−460: Hurricane Katrina: Comprehensive Policies and Procedures Are Needed to Ensure Appropriate Use of and Accountability for International Assistance (Report).** In response to Hurricane Katrina, countries and organizations donated to the United States government cash and in−kind

donations, including foreign military assistance. The National Response Plan establishes that the Department of State is the coordinator of all offers of international assistance. The Federal Emergency Management Agency within the Department of Homeland Security (DHS) is responsible for accepting the assistance and coordinating its distribution. In light of widespread congressional and public interest in U.S. agencies' accountability in receiving and distributing assistance to hurricane victims, this report is one of several initiated under the authority of the Comptroller General to review the federal government's response to Hurricane Katrina. It examines (1) the amount and use of internationally donated cash, and (2) the extent to which federal agencies have adequate policies and procedures to ensure proper accountability for the acceptance and distribution of that assistance. The Government Accountability Office (GAO) makes recommendations designed to improve the policies, procedures, planning, and oversight of international cash and in−kind donations to the U.S. government in response to disasters. The Department of Defense and DHS generally agreed with GAO's recommendations and cited actions being taken.
Highlights: http://www.gao.gov/highlights/d06460high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−460

28. *April 06, Government Accountability Office* — **GAO−06−600T: Hurricane Katrina: Policies and Procedures Are Needed to Ensure Appropriate Use of and Accountability for International Assistance (Testimony).** In response to Hurricane Katrina, countries and organizations donated to the United States government cash and in−kind donations, including foreign military assistance. The National Response Plan establishes that the Department of State is the coordinator of all offers of international assistance. The Federal Emergency Management Agency within the Department of Homeland Security (DHS) is responsible for accepting the assistance and coordinating its distribution. The Government Accountability Office's (GAO) testimony covers (1) the amount and use of internationally donated cash and (2) the extent to which federal agencies with responsibilities for international in−kind assistance offered to the United States had policies and procedures to ensure the appropriate accountability for the acceptance and distribution of that assistance. In its related report, (GAO−06−460) GAO made six recommendations designed to improve the policies, procedures, planning, and oversight of international cash and in−kind donations to the U.S. government in response to disasters. In comments on the draft report, the Department of Defense and DHS generally agreed with GAO's recommendations and cited actions being taken to further refine processes and procedures for managing international disaster donations to the United States.
Highlights: http://www.gao.gov/highlights/d06600thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−600T

29. *April 05, Federal Computer Week* — **Louisiana governor creates interoperability committee.** Louisiana's governor has formed an executive committee that comprises state and local officials to oversee establishment of a modern statewide interoperable and reliable communications system for emergency response. Governor Kathleen Blanco issued an executive order last week forming the 27−member committee. The new executive order supersedes a similar one issued in early February that created an interoperability committee.
Source: http://www.fcw.com/article93969−04−05−06−Web

30. *April 05, Federal Computer Week* — **Survey: Interoperability tops priority list for state homeland security directors.** Homeland security directors from state governments identified

interoperable communications for first responders as their top priority for the second year in a row, according to a new National Governors Association (NGA) survey. According to the survey, homeland security directors also identified developing a state intelligence fusion center, coordinating state and local agency efforts, and identifying and protecting critical infrastructure as their other top priorities. The new survey also reflects two new state priorities: improving preparedness and response to natural disasters and planning for a possible influenza pandemic. NGA's Center for Best Practices conducted its second annual survey between December 2005 and January 2006 with the 55 homeland security directors from U.S. states, territories and commonwealths.
NGA's survey: http://www.nga.org/Files/pdf/0604HLSDIRSURVEY.pdf
Source: http://www.fcw.com/article93971−04−05−06−Web

[Return to top]

Information Technology and Telecommunications Sector

31. *April 05, Government Computer News* — **Trends in botnets: smaller, smarter.** Some recent statistics on e−mail traffic provide more evidence of the trend toward smarter, more targeted online attacks. Botnets −− networks of compromised computers taken over by spammers and hackers −− are getting smaller. Rather than hundreds of thousands of zombie computers spitting out unwanted e−mail and malicious code, they now consist of tens of thousands. “They stay under the radar for longer,” said MessageLabs chief technology officer Mark Sunner. “The return is still equal, if not greater, because the attacks are more targeted.” Sunner said he expects continued refinement in attacks to be the distinguishing trend this year for spammers, hackers and purveyors of malicious code.
Source: http://www.gcn.com/online/vol1_no1/40334−1.html

32. *April 05, Information Week* — **Microsoft: Social engineering is just as dangerous as software vulnerabilities.** Attacks that rely on "social engineering" tricks to fool users into visiting malicious Websites are just as dangerous as any that exploit software vulnerabilities, Microsoft security researcher Matt Braverman, argued. According to Braverman, a program manager with Microsoft's Anti−Malware Technology Team, data from the group's February update of its Malicious Software Removal Tool discovered an unusually high number of Alcan.b worms on users' PCs. "Alcan.b does not exploit any software vulnerabilities. Instead, it spreads through popular peer−to−peer applications and its prevalence is likely due to effective social engineering...Threats like this reinforce the idea that malware that exploits user weakness can be as dangerous as those threats which exploit software vulnerabilities," claimed Braverman.
Source: http://www.informationweek.com/news/showArticle.jhtml;jsessionid=3ISV1FYRRBVOWQSNDBGCKHSCJUMEKJVN?articleID=184429007

33. *April 05, PC World* — **Security fears hamper mobile devices.** Around 60 percent of businesses are shying away from deploying mobile devices primarily due to security concerns, according to a new survey conducted by the Economist Intelligence Unit and commissioned by security vendor Symantec. Executives at 240 organizations worldwide were interviewed. One in five organizations said they have sustained financial losses due to an attack on mobile data platforms. Businesses also said they rated threats from viruses as the same or greater on mobile

devices than on a fixed network.
Source: http://www.pcworld.com/news/article/0,aid,125319,00.asp

34. *April 05, Secunia* — **SGI advanced Linux environment multiple updates.** SGI has issued a patch for SGI Advanced Linux Environment. This fixes some vulnerabilities and a security issue, which can be exploited by malicious, local users to gain escalated privileges and read arbitrary cron files, and by malicious people to bypass certain security restrictions, potentially cause a denial−of−service, and compromise a vulnerable system.
For a complete list of vulnerable products please see: http://secunia.com/advisories/19532/
Solution: Apply patch 10291 for SGI ProPack 3 Service Pack 6. http://support.sgi.com/
Source: http://secunia.com/advisories/19532/

35. *April 04, Information Week* — **Rhode Island prepares for statewide wireless network.** An ambitious effort to create a wireless broadband network to cover the entire state of Rhode Island is moving towards the implementation stage as two trial networks are currently being established. The non−profit Rhode Island Wireless Innovation Networks (RI−WINS) is in the process of deploying a base station at the Brown University Science Laboratory and another in Newport, said Bob Panoff, who has been spearheading the RI−WINS effort. The network, planned to cover the state's more than 1,000 square miles, is tentatively planned to be in operation in 18 to 24 months.
Source: http://www.informationweek.com/news/showArticle.jhtml?articleID=184428680&subSection=Breaking+News

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT is aware of an active exploitation of a cross site scripting vulnerability in the eBay website. Successful exploitation may either allow an attacker to obtain sensitive data from stored cookies or redirect auction viewers to phishing sites where further disclosure of login credentials or personal information can occur. For more information about the reported vulnerability can be found in the following:

CA−2000−02 CERT Advisory: Malicious HTML Tags Embedded in Client Web Requests http://www.cert.org/advisories/CA−2000−02.html

VU#808921 US−CERT Vulnerability Note: eBay contains a cross site scripting vulnerability http://www.kb.cert.org/vuls/id/808921

US−CERT recommends the following:

Disable Scripting as specified in the Securing Your Web Browser document at URL:

http://www.us−cert.gov/reading_room/securing_browser/#how_to_secure

The Malicious Web Scripts FAQ information at URL:http://www.cert.org/tech_tips/malicious_code_FAQ.html#st eps

Validate web site addresses as described in the eBay Spoof Email Tutorial information at URL: http://www.microsoft.com/technet/security/advisory/917077.mspx

ST04−014 US−CERT Cyber Security Tip document at URL: http://www.us−cert.gov/cas/tips/ST04−014.html

ST05−010 Validate web site certificates as described in US−CERT Cyber Security Tip document at URL: http://www.us−cert.gov/cas/tips/ST05−010.html

Phishing Scams
US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are being targeted. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft−ds), 32459 (−−−), 41170 (−−−), 3525 (−−−), 44331 (−−−), 32768 (HackersParadise), 20117 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer